# SHELL

TP 1

Sudoers

Analyse de logs

charles.meunier@u-bourgogne.fr

# Objectifs

Découvrir les bases du Shell sous Linux à travers des exercices pour :

- Gérer les utilisateurs d'une machine
- Extraire des informations depuis un fichier

# Retour à la gestion des utilisateurs

### adduser / useradd [10 minutes]

- Pour commencer, vous allez créer deux utilisateurs avec deux méthodes différentes : Utilisez la commande « adduser » pour créer l'utilisateur « user1 » et « useradd » pour créer l'utilisateur « user2 ».

| Utilisateur | Mot de passe |
|---|---|
| user1 | pwduser1 |
| user2 | pwduser2 |

- Quelles sont les différences entre ces deux commandes ?
- Connectez-vous en tant que « user1 », puis en tant que « user2 ». Qu'observez-vous ?
- Quelle commande permet de définir le mot de passe d'un utilisateur ?
- Supprimer les deux utilisateurs précédents.

### Squelette de compte utilisateur [10 minutes]

Lorsque vous gérez un parc informatique important, il est intéressant de pouvoir fournir une structure de dossiers initiale identique pour chaque utilisateur. Par exemple, sous Windows, lorsque vous créez un nouveau compte, vous disposez de toute une arborescence : « Mes documents », « Mes images », …

Voyons à présent comment automatiser ceci, car vous vous doutez bien que l'administrateur système à d'autres choses plus intéressantes à faire.

- Créez les dossiers « documents », « images », « vidéos » dans le dossier « /etc/skel »
- Créez également un fichier « bienvenue.txt » contenant le texte « Bienvenue à l'ESIREM !»
- Créez un nouvel utilisateur « user3 » en utilisant la commande « adduser ».
- Que remarquez-vous dans le dossier personnel de l'utilisateur « user3 » ?

### Sudoers [10 minutes]

Vous l'avez vu à plusieurs reprises, il est possible d'invoquer les droits administrateurs afin d'effectuer certaines tâches, sans être connecté en tant que « root ».

- Connectez-vous avec l'utilisateur précédemment créé (user3).
- Créez un nouvel utilisateur « user4 ».
- Que remarquez-vous ?

Pour invoquer les droits administrateur, l'utilisateur doit faire partie d'une sorte de ligue des justiciers, de gang sympa des cités, groupe que l'on appelle dans le jargon les « sudoers » : ceux qui peuvent appeler la commande sudo. Et oui, pouvoir améliorer ou flinguer le système ça se mérite.

- Revenez sur le compte « esirem »
- Ajoutez l'utilisateur « user3 » au groupe « sudo ». Comment ? Mais si, rappelez-vous, vous avez galéré au premier TD !
- Connectez-vous à nouveau avec « user3 » et essayez de créer un nouvel utilisateur.

## Gestion des logs

Les fichiers de journalisation (logs) permettent de mémoriser certains événements normaux ou indésirables survenus durant le fonctionnement d'une application ou l'exécution d'un script. Ils contiennent souvent un grand volume d'information qu'il est difficile, pour un humain, de traiter.

### Récupération du fichier log à traiter [5 minutes]

Afin de travailler dans des conditions réalistes, vous allez récupérer le journal des connexions entrantes du serveur apache qui gère le site de La Marmotte.

- Utilisez la commande « wget » pour récupérer le fichier situé à l'adresse suivante :

  https://www.lamarmotte.info/wp-content/uploads/2022/10/access.log

- Affichez le contenu du fichier (« cat » ou « less »).

Vous commencez à cerner l'importance de traiter ce genre de fichier autrement qu'en le parcourant ligne après ligne ? Et là, on parle d'un log de La Marmotte, pas d'Amazon…

### Traitement du fichier [25 minutes]

Voyons à présent ce que l'on peut tirer de ce fichier.

- Combien de lignes contient ce fichier ? Dites-moi que vous n'allez pas les compter à la main. Eh oui, un wc, c'est toujours utile !
- Afficher les requêtes effectuées par l'utilisateur ayant l'adresse IP « 78.219.34.20 » (grep).
- Combien de requêtes avez-vous trouvées ?
- A présent, parmi toutes les informations que nous donne ce log, n'affichez que les adresse IP des utilisateurs. La commande « cut » vous permet de découper une ligne selon un délimiteur et de n'afficher que certains des champs ainsi trouvés.
- On voit qu'une même adresse IP peut apparaître plusieurs fois. Utiliser la commande « sort » avec l'option « -u » pour supprimer les doublons.
- Combien d'adresse IP différentes trouvez-vous ?
- Enfin, pour voir ceux qui s'intéressent au cours, extrayez les IP des élèves qui ont téléchargé (**GET**), **ce mois-ci**, le dernier CM de Shell : **CM-3-Scripts-Shell.pdf**.

### Détection des attaques [30 minutes]

Tout service exposé à Internet est régulièrement victime d'attaques tentant d'exploiter des failles de sécurité. Parmi les plus fréquentes, on retrouve les attaques « Brut force » qui consistent à se connecter en utilisant tous les mots de passe possible et imaginable les uns à la suite des autres. Ce type d'attaques n'est, en général, pas très efficace et facilement détectable du fait du grand nombre de requêtes que cela produit.

- Réalisez un script qui analyse le fichier de log étudié précédemment et qui affiche la liste des adresses IP suspectes, c'est-à-dire qui accède au script « wp-login.php » ou qui réalise un nombre de requêtes anormalement élevé : supérieur à 100

**Ça pourrait vous aider…**

- La commande `uniq -c` affiche de manière unique les valeurs d'une liste ainsi que leur nombre d'occurrences.
- Pour initialiser un tableau, on utilise la syntaxe suivante

```
declare -a array=(un deux trois)
```

- Pour scinder les mots (séparés par un espace) d'une chaine de caractères, on utilisera donc la syntaxe suivante :

```
declare -r chaineDeCaracteres="un deux trois"
declare -a tableau=($chaineDeCaracteres)
```

- Votre enseignant peut aussi avoir deux trois infos. Posez-lui des questions 😉